CUSERID

Never rely on username for security - (Function is obsolete)

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-22

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4441 bytes

<table>
<tr><td><b>Attack Category</b></td><td>• Privilege Exploitation</td></tr>
<tr><td><b>Vulnerability Category</b></td><td>• Access Control</td></tr>
<tr><td><b>Software Context</b></td><td>• Authorization</td></tr>
<tr><td><b>Location</b></td><td>• stdio.h</td></tr>
<tr><td><b>Description</b></td><td>cuserid(char *s) generates a character-string representation of the user name corresponding to the effective user ID of the process. If s is a NULL pointer, this representation is generated in an internal static area, the address of which is returned. Otherwise, s is assumed to point to an array of at least L_cuserid characters; the representation is left in this array. The constant L_cuserid is defined in the <stdio.h>header file.
Never rely on username for security.
cuserid() should be considered obsolete. This function has been or will be deprecated in several systems (e.g., HPUnix. ISO POSIX-1). Additionally this function has changed capability within a given OS (HP).</td></tr>
<tr><td><b>APIs</b></td><td><table><tr><th>Function Name</th><th>Comments</th></tr><tr><td>cuserid</td><td></td></tr></table></td></tr>
<tr><td><b>Method of Attack</b></td><td></td></tr>
<tr><td><b>Exception Criteria</b></td><td></td></tr>
<tr><td><b>Solutions</b></td><td><table><tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr><tr><td>Generally applicable</td><td>Convert to getpwuid (getuid()), getpwuid (geteuid()), or getlogin(), depending on</td><td>Effective.</td></tr></table></td></tr>
</table>

[1] http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

	which user name is desired.
Signature Details	char *cuserid(char *s);

Examples of Incorrect Code	// The function is deprecated
	char *t_userid;
	#ifdef __GNUC__
	(int)t_userid = cuserid((char *)
	NULL);
	#else
	t_userid = cuserid((char *)
	NULL);
	#endif /*

Examples of Corrected Code	void user_name(void)
	{
	/* See the getpwuid man page
	* for a description of the
	* structure.
	*/
	struct passwd *passwd;
	/* Get the uid of the running
	* process and use it to get
	* a record from /etc/passwd
	*/
	passwd=getpwuid(getuid());
	printf("Users Real name is %s\n",
	passwd->pw_gecos);
	}

Source References	• cuserid manpage • HP-UX Reference. cuserid(3S[2]
Recommended Resource	
Discriminant Set	**Operating System**: • Windows **Languages**: • C • C++

Cigital, Inc. Copyright

[1] mailto:copyright@cigital.com

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.